"Enhanced the Security for WSN Protocols from Attacks & Countermeasures"

A Synopsis

Submitted in

Partial fulfillment for the degree

of

Doctor of Philosophy

(Computer Science)

Supervised by

Dr. Banta Singh Jangra

Submitted by

JV'n Ms. Vijeta Kumawat

Department of Computer Science and Information Technology
Faculty of Engineering & Technology
Jayoti Vidyapeeth Women's University
Jaipur (Rajasthan), India
May, 2011

INTRODUCTION

Wireless Sensor Networks is a collection of sensor nodes ranging from hundreds to thousands for sensing the environment, collection of desired data from sensors and transmit these collected data to a central point which is known as base station and the network is called wireless sensor network. Wireless Sensor Networks possess a wide range of applications such as in environmental condition measurement such as, weather forecasting and prediction, determining temperature, sound, wave, and military applications. In wireless sensor networks, each sensor device runs by own battery for the energy consumption so we can say that battery is the prominent resource in wireless sensor networks. In current scenario, it is a very challenging or hard task to replace or recharge these batteries of sensor nodes because nodes have mobility and these are deployed in rarest areas. So, the routing protocols chosen for wireless sensor network must be energy efficient. Introduction of malicious fictional activity is another research issues in wireless sensor network from it's security point of view. Due to malicious activity, the communication of sensor node and center location may be interrupted or data may be loss or theft [1, 2].

BACKGROUND

Routing in Wireless Sensor Networks

Wireless sensor networks have certain constraints such as, there is no fixed organization, links are untrustworthy and sensor nodes may fail at any time due to the lack of energy resource. Routing protocol requires few energy saving techniques, due to the limited energy constraint faced by the sensor nodes [3]. That is why, wireless sensor networks need different routing protocols unlike other traditional static networks such as MANET'S. Routing protocols are categorized in seven different types for sensor networks.

1. Data Centric Protocols

In address based protocols, sensor nodes independently transfer data directly to the base station without involvement of middle nodes. While in the case of data centric protocols, the middle nodes performs some functions on the data receiving from other sensor nodes and then data is send by middle to the base station. This technique moderates the consumption of power in the transfer of sensed data. Rumor Routing, Active Query Forwarding in Sensor Networks

(ACQUIRE), Cougar, Energy-Aware Data-Centric Routing protocol (EAD), Sensor Protocols for Information via Negotiation (SPIN) are few examples of data centric protocol.

2. Location Based Routing Protocols

In location based routing protocols, sensor nodes are deployed at diverse locations. The detail about the location of a node is to be used in order to calculate the distance of two sensor nodes and this distance is used further for calculating the energy usage in networks. Example of location based routing protocols are Geographic Random Forwarding (GeRaF), Geographic and Energy-Aware Routing (GEAR), Small Minimum-Energy Communication Network (SMECN), Geographic Adaptive Fidelity (GAF), Minimum Energy Communication Network (MECN) [4].

3. Mobility-Based Protocols

In these protocols, the sensor nodes and the sink node both are movable and in this case, prerequisite is to design an energy efficient routing protocols that could ensure the successful data delivery from the source sensor nodes to the base station. Examples of Mobility-based Protocols: Scalable Energy-Efficient Asynchronous Dissemination (SEAD), Joint Mobility Routing Protocol and Data MULES Based Protocol [5].

4. Hierarchical Protocols

In hierarchical based routing protocols, the sensor nodes are grouped into a cluster on the basis of distance and a node from each cluster is chosen as a cluster head. The sensor nodes of a cluster send their sensed data to cluster head of their cluster. This cluster head can applied some function on receiving data from different sensor node and after completing the process, this aggregated data is sent to the base station. The aggregation functions are applied on a cluster head rather than each sensor node so the repetition of aggregation operation is reduced and transmission to cluster head is closer than base station which is far from sensor node compared to cluster head. That's why the energy consumption is less in the hierarchical routing protocols. Example of hierarchical based routing protocols: Hybrid, Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN), Energy-Efficient Distributed Clustering (HEED), Low-Energy Adaptive Clustering Hierarchy or LEACH[6].

5. Quality of service Routing Protocols

Along with energy efficiency factor, factor of quality of service should also be taken care of. It is calculated in respect to the packet delivery ratio, end to end delay, speed and others parameters of quality of services[7].

6. Heterogeneity based routing Protocols

Basically, there are two types of nodes. The first category of nodes is line powered sensor nodes that have no energy constraints and hence, energy of these sensor nodes is used to the largest extent possible. The second category is battery powered nodes that have firm energy constraints. So, energy for these nodes should be used efficiently by decreasing the data computation and communication loads. Examples of heterogeneity-based routing protocol: Cluster Head Relay Routing (CHR) and Information-Driven Sensor Query (IDSQ)[8].

7. Multi Path-Based Protocols

A sensor node sends it data using the selection of the shortest path to base station in the single path based routing while in contrary every sensor node discovers the first k possible shortest routes to base station and send data to these possible routes by distributing uniformly in multi path routing protocol[9].

LEACH (Low Energy Adaptive Clustering Hierarchy) Routing Protocol

LEACH is one of the existing hierarchical routing protocols in wireless sensor networks. In this protocol, all the sensor nodes are structured in the form of clusters. In each cluster, one node acts as a local base station and is appointed as the cluster head for that specific cluster. Each sensor node can contact its corresponding cluster head only. As, all the cluster members are communicating with a single node, that is, their cluster head, so, the cluster head needs more computation and transmission as compared to the member sensor nodes. So if cluster heads are permanent, they would die rapidly. To avoid this problem, LEACH protocol uses randomized cluster head rotation among sensor nodes, so that the battery of all the sensor nodes is consumed equally. As a result, this increases the overall lifetime of wireless sensor networks. LEACH protocol uses local data fusion technique at each cluster head. This technique compresses the data being sent to the base station by each cluster head[10].

Possible attacks on LEACH

LEACH is an energy efficient protocol used in wireless sensor networks, but it can be susceptible to few attacks. Following are the possible attacks [11] on LEACH protocol in wireless sensor networks.

1. Selective Forwarding Attack

In selective forwarding attack, the malicious node place itself in the path of data and refuses to forward some data by dropping the data. It forwards some data and drops the rest of it. In contrary, the black hole attack is less harmful attack because the malicious nodes drop all the data received on it and it can be easily detected. But in selective forwarding attack,the malicious nodes selectively forward some data and drops rest of the data, making it impossible to detect the malicious activities .In LEACH protocol, when malicious node becomes cluster head, it drops some data coming from the member nodes, which is destined to the base station. This packet dropping can be done on the basis of node ids, time intervals, packet type or packet size etc[12].

2. Sybil Attack

In a Sybil Attack, the malicious node illegally generates many identities to the nodes in the sensor networks. This is done either by creating new false identities or imposing identities of other nodes in the network. This ultimately affects the overall performance of the network as wireless sensor networks have strict energy constraints and the malicious node is wasting the energy resource in one way or the other. The Sybil node takes advantage of the identities of a normal node, using a single node as many times. This may results in various problems in the network such as traffic congestion, more energy consumption, reduced network lifetime, packet dropping etc.

3. Hello Flooding Attack

In many routing protocols, it is sometimes required to transmit hello messages to the neighbor nodes. But some malicious nodes send continuously hello messages to all other nodes in the

network. So there may be a flood of hello messages, which results in tremendous traffic congestion in the network and collisions may occur. In wireless sensor networks, the malicious nodes would consume more energy of other nodes as it sends hello messages repeatedly and hence energy is consumed unnecessarily. In the case of LEACH protocol,the malicious node may send large number of false messages and it may results in additional wastage of huge amount of energy of other nodes in the network, so the lifetime of the whole network is reduced tremendously.

OBJECTIVE OF THE STUDY

The objective of the study is to enhance the security for WSN protocols from attacks & countermeasures, so that data can be transmit in a secure manner in the network. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Data delivery. The secondary goals are efficient power consumption.
The objective for this research work is to analyze the performance of communication network due to introduce of Selective Forwarding Attack in LEACH routing protocol of wireless sensor network with changing the parameters of number of cluster head and determined the detection and removal of select forwarding attack in LEACH routing protocol of communication network and then to analyze the performance of LEACH routing protocol in the presence of selective forwarding attack.

Characteristics and Research Issues in Wireless Sensor Network

Wireless sensor networks have some different characteristics [13] as compared to the previous wireless networks such as Mobile Ad Hoc Networks (MANET) and cellular system. Its attributes are as follows:

1. The density of sensor nodes in wireless sensor networks is higher than the density of mobile nodes in MANET. So, it allows sensor nodes to have better sensing capabilities.

2. Sensor node has very limited energy sources, computation and memory capabilities.

3. Sensor nodes are highly dependent upon battery. So, if the battery of sensor node is fully discharged, then that particular sensor node may fail, replacing and recharging its battery is very hectic process due to the difficult deployment of sensor nodes.

In wireless sensor networks, each sensor device runs by own battery for the energy consumption so battery is the prominent resource in wireless sensor networks and it is a very challenging or hard task to replace or recharge the these battery of sensor devices because these node are deployed in remote areas and may have mobility in some applications.

So routing protocols and data transfer should be efficient in case of overall energy consumption for wireless sensor networks so that it should enhance the overall life of sensor network communication. From security point of view, there is a possibility of attack by intruders on routing protocols in wireless sensor networks and this may possibly degrade the performance of the entire network. Low Energy Adaptive Clustering Hierarchy or LEACH is a routing protocol which uses randomized cluster rotation scheme and is energy efficient algorithm in which energy load is distributed among all sensor nodes.

Wireless sensor networks are classified in two categories: (1) Heterogeneous wireless sensor networks and (2) Homogeneous wireless sensor networks. In heterogeneous sensor networks, a sensor node is different in the factor such as receiving power, transmission power, energy, computational capability etc. while in homogeneous wireless sensor networks all sensor nodes have same in compared to other nodes in terms of above factors.

REVIEW OF LITERATURE

An energy efficient scheme is very essential for network communication in wireless sensor networks. The basic purpose behind this research work till date is basically concentrated on efficient network communication and decrease consumption of energy in network communication so that the overall network lifetime could be enhanced with same level of fixed level of battery charge. There are various routing techniques which were used in the previous research work but the clustered based routing technique turns out to be the most dominant, promising and scalable technique. For decreasing the total consumption of energy in network

communication, a node is determined as a cluster head by evaluating the best estimated probability method [14].

Heinemann et. al. [15] proposed a technique for wireless sensor networks based on hierarchical clustering routing, which is called as LEACH routing protocol. This routing approach acts a formation of distributed randomized cluster.

Ben Alla Said *et al.* [16] proposed a scheme called Improved and Balanced LEACH (IB-LEACH). This is a heterogeneous-energy protocol that provides a new mechanism to decrease probability of failure nodes and to extend the time interval before the death of the first node and it extend the lifetime of heterogeneous WSNs. This is very important for many applications. The impact of heterogeneity of hierarchically clustered nodes in wireless sensor networks is observed, in terms of the energy. In this scenario, the high energy nodes are known as NCG nodes (Normal node/Cluster Head/ Gateway). These nodes are elected as "cluster heads" which aggregate the data sent by their cluster members. Cluster nodes are transmitted to the chosen "Cluster Head". Minimum communication energy is required for this transmission that will finally minimize the energy consumption of cluster head and reduce the probability of failure nodes. According to this simulation results new protocol is additional energy efficient and more effective for extending the network life time and have stability period compared to LEACH and SEP.IB-LEACH is an addition of the LEACH. It expands the stable region of the clustering hierarchy and also decreases chances of failure nodes using the characteristic parameters of heterogeneity in networks. In this type of network, high energy nodes are known as NCG nodes (Normal node or Cluster Head or Gateway). These nodes are works as "cluster heads" and these nodes aggregate the data of their cluster members and then transmit it to the chosen "Gateways". This method needs the minimal communication energy I order to reduce the energy consumption by each cluster head. It decrease the failure probability and increase the lifetime of the network. These results shows that the IB-LEACH have better performance as compared to SEP and LEACH in both heterogeneous and homogeneous environments. In this method, the NCG nodes are distributed randomly and fixed.

LIANG Ying *et. al*[17] said that a wireless network consist a large number of small sensors with limited battery power that can be an effective tool for gathering data in a variety of

environments. Clustering sensors into groups, so that sensors interact with cluster-heads and send information only to them, and then the cluster-heads communicate the aggregated information to the base station, may save energy. He propose an optimal energy- adaptive clustering algorithm which is motivated from the LEACH protocol .In this optimization of LEACH's random cluster-head selection algorithm is done to ensure the balanced energy depletion over the whole network thus prolongs the network lifetime.Here is the discription of modification of LEACH's random cluster-head selection algorithm by synthetically considering two additional parameters including the remaining energy level and the dissipated energy level for each node. Since evenly distributes energy-usage among the nodes in the network, our optimal cluster-head selection could save a lot of communication energy of sensor nodes, thus increase the lifetime and quality of the system. Simulation shows that the distribution of dead nodes using this proposed algorithm is more even than that using LEACH. Moreover, algorithm outperforms LEACH by about 20% to 35% when 1%, 50%, 100% of nodes die for different network sizes and topologies

Sampath Priyankara *et. al* [18] proposed a clustering method for wireless sensor networks with heterogeneous node types which select cluster heads considering not only transmission power and residual energy of each node but also those of it's adjacent nodes .Recently, sensor network systems are gradually moving into heterogeneous designs, incorporating a mixture of variety in sensor nodes type also. Some routing protocols have been suggested for sensor networks but most of them did not consider the non-uniform energy drainage caused by many-to- one traffic. But for his work, Simulations show that this method significantly increases network lifetime and also maintains high coverage rate in comparison with existing methods. In this they proposed a clustering method for WSNs with heterogeneous node types, which select cluster heads considering not only the performance of a certain node but also that of its adjacent nodes. The simulations validate the result that this clustering method is able to prolong the lifetime in heterogeneous network environment. Now they have considered a limited number of aspects of a sensor network. But future work would explore coverage problems and residual energy concerned rooting of sensor networks. The possibility of multiple sinks located in geographically different locations should also be considered. Another important issue to be explored is a heterogeneous network model where the difference between the sensors is not only the difference in initial energy and communication range, but also in their processing

capabilities, and thus the consideration of energy consumption in data processing (compression, fusion, etc.)

WenLiu *et al.* [19] propose an improved algorithm for cluster head election of LEACH algorithm in Wireless Sensor Network(WSN) based on LEACH from point of view that regional energy balance of the network. This algorithm can select the node that has more remaining energy to serve as the cluster head(CH). Meanwhile,the selection done by sensor nodes to choose the CHs, will depend on not only the distance between the Chs and the sensor nodes , but also the capacity of the CHs to join. Simulation results show that the proposed algorithm is effective in balancing the network energy consumption and prolonging the network lifetime. For the cluster head election in LEACH algorithm without consideration of energy factors and the uneven distribution of member nodes that all cluster head have, an energy balance algorithm based on LEACH is proposed in this work. Simulation results also show that the improved algorithm can balance the energy consumption of the entire network, delay the time that FND in the network and prolong the lifetime of the entire network effectively. But in the modified algorithm part of all cluster head need to consume extra energy to receive the control message from the sink node. This should be improved in the future.

Young Ki Kim *et al.*[20] said that Wireless sensor networks are networks consisting of nodes with sensors to monitor physical or environmental conditions. If a malicious node is present on a route by which packets are forwarded, attackers can easily perform selective forwarding attacks by simply dropping packets. Selective forwarding attacks can be serious threats on many applications including networks for military surveillance and health-care monitoring. Previous counter measures to selective forwarding attacks cannot identify malicious nodes or require time synchronization. In this scheme, they present a detecting scheme which identifies malicious nodes delivering selective forwarding attacks without the need for time synchronization, security against sinkhole attacks in which attackers try to attract more traffic to malicious nodes. Selective forwarding attacks can be serious threats on wireless sensor networks. However, previous countermeasures required time synchronization or high communication overhead. But in this an efficient detection scheme against selective forwarding attacks is used. This scheme essentially detects malicious nodes for each possible scenario. By sending acknowledgements to the base station in a cumulative manner, our scheme eliminated

the need of time synchronization for authentication. For the best of knowledge, CADE is the first scheme identifying nodes conducting selective forwarding attacks without broadcast authentication. In terms of communication overhead, our scheme is more efficient than typical multipath schemes; while the whole data is sent through multiple paths in multi-path schemes, only small packets indicating presence of data are transmitted through multiple paths in CADE. Further, these indication packets are not even necessary in networks where nodes periodically report to the base station. In addition, by utilizing an existing routing protocol which is secure against sinkhole attacks, our scheme also provides security against sinkhole attacks.

METHODOLOGY

I have used Network Simulator 2 (version 2.34) in my experiments.

Network Simulator 2

Network Simulator (Version 2), known as NS2 [23], is an event-driven simulation tool which is very useful for studying and simulating the nature of communication networks. NS2 provides the network environment, where user can simulate the networking tasks and analyzes the network performance. In NS2, user can simulate wired as well as wireless network functions and protocols like routing algorithms, TCP, UDP and also security aspects can be simulated using this. In general, NS2 provides users with a way of particularising such network protocols and simulating their corresponding behaviors.

Figure 1 shows the basic architecture of NS2. In NS2 there is an executable command "ns" which takes a Tcl simulation scripting file as input and simulation trace file is generated as output which is used to plot graph and to create animation.

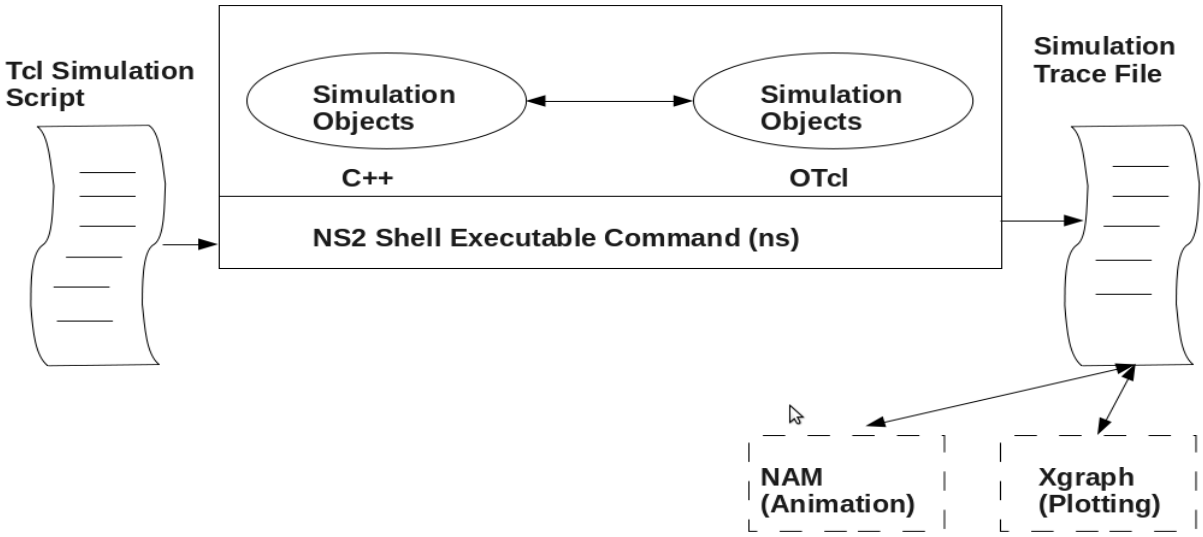

Figure 1: Block Diagram of NS2 Architecture

NS2 consists of two key languages, that is, C++ and Object-oriented Tool Command Language (OTcl). The C++ is used to define its inside's mechanism (i.e. a backend) of the simulation, the OTcl sets up simulation by assembling and configuring the objects as well as planning discrete events (i.e. a frontend). TclCL is an interface that is used to link C++ and OTcl together. Mapped to a C++ object, variables in the OTcl domains are sometimes called to as handles. Theoretically , a handle is just a string (e.g. "_010") in the OTcl domain and does not carry any functionality. Instead, the functionality (e.g. receiving a packet) is stated in the mapped C++ object (e.g. of class Connector). A handle acts as a frontend in the OTcl domain, which interacts with users and other OTcl objects. It may explain its own procedures and variables to facilitate the interaction. Instance procedures (instprocs) is collection of the member procedures and variables in the OTcl domain and instance variable (instvars), respectively [21].

After simulation, NS2 generates text-based simulation results in the form of trace files. To interpret these results graphically and interactively, tools such as NAM (Network Animator) and Xgraph are used.

REFERENCE

[1] Thorat, Meera A., and Vivek S. Deshpande. "Assessment of fairness against quality of service parameters in wireless sensor networks." In *Wireless and Optical Communications Networks (WOCN), 2016 Thirteenth International Conference on*, pp. 1-5. IEEE, 2016.

[2] Anbhazhagan, P., and S. Nagarajan. "A Novel Cluster Head Selection for Enhancing the Lifetime in Wireless Sensor Networks." *Networking and Communication Engineering* 8, no. 1 (2016): 6-10.

[3] O. Younis and S. Fahmy. Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. In IEEE Transactions on Mobile Computing, volume 3, pages 366–379, April 2004.

[4] Raghavenda Lindsey S. Pegasis:power efficient gathering in sensor information systems. In In Proc of the IEEE Aerospace Conf. New York, IEEE Press, pages 1125–1130, 2002.

[5] Li Qing ,Qingxin Zhu, Mingwen Wang, "Design Of A Distributed Energy-Efficient Clustering Algorithm For Heterogeneous Wireless Sensor Networks" , 14 February 2006

[6] Sampath Priyankara, Kazuhiko Kinoshita, Hideki Tode, KosoMurakami,"A Clustering Method For Wireless Sensor Networks With Heterogeneous Node Types" 2009 IEEE.

[7] Ali Hosseinalipour, Davood Keykhosravi, Abbas Mirzaei Somarin "New Hierarchical Routing Protocol For Wsns", 2010 IEEE.

[8] Haosong Gou, YounghwanYoo, "An Energy Balancing LEACH Algorithm For Wireless Sensor Networks", 2010 IEEE

[9] Desalegn Getachew Melese, Huagang Xiong, Qiang Gao, "Consumed Energy As A Factor For Cluster Head Selection In Wireless Sensor Networks",2010 IEEE

[10] Wenliu, Zhiyuan Ma, Zhongliang Deng, Lianmingxu, " Energy Balance Algorithm Based On LEACH", 20 10 IEEE

[11] Shamneesh Sharma, Robin Prakash Mathur, Dinesh Kumar, "Enhanced Reliable Distributed Energy Efficient Protocol For WSN", 2011 IEEE

[12] Vivek Katiyar, Narottam Chand, Surender Soni, "Clustering Algorithms For Heterogeneous Wireless Sensor Network: A Survey", International Journal Of Applied Engineering Research, Dindigul, Volume 1, No 2, 2010

[13] E.J. Coyle S. Bandyopadhyay. An energy efficient hierarchical clustering algorithm for wireless sensor networks. In IEEE INFOCOM, pages 1713–1723, April 2003.

[14] Kumari, Neelu, Sandeep Kumar Gupta, Rajni Choudhary, and Shubh Laxshmi Agrwal. "New performance analysis of AODV, DSDV and OLSR routing protocol for MANET." In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 33-35. IEEE, 2016.

[15] Wendi B. Heinzelman, Anantha P. Chandrakasan, HariBalakrishnan, "An Application Specific Protocol Architecture For Wireless Microsensor Networks", IEEE Transactions On Wireless Communications, Vol. 1, No. 4, October 2002.

[16] C. P. Low, C. F. J. M. Ng, and N. H. Ang., "Efficient load-balanced clustering algorithms for wireless sensor networks". In Elsevier Computer communications, pages 750–759, 2007.

[17] Liang, Ying, and Haibin Yu. "Energy adaptive cluster-head selection for wireless sensor networks." In *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pp. 634-638. IEEE, 2005.

[18] Priyankara, Sampath, Kazuhiko Kinoshita, and Koso MURAKAMI. "A clustering method for wireless sensor networks with heterogeneous node types." *IEICE transactions on communications* 94, no. 8 (2011): 2254-2264.

[19] Liu, Wen, Zhiyuan Ma, Zhongliang Deng, and Lianming Xu. "Energy Balance Algorithm based on LEACH." In *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pp. 681-684. IEEE, 2010.

[20] Kim, Young Ki, Hwaseong Lee, Kwantae Cho, and Dong Hoon Lee. "CADE: Cumulative acknowledgement based detection of selective forwarding attacks in wireless sensor networks." In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2, pp. 416-422. IEEE, 2008.

[21] Fco. Javier Atero, Juan Jose Vinagre, Julio Ramiro, Mark Wilby, "A Low Energy And Adaptive Routing Architecture For Efficient Field Monitoring In Heterogeneous Wireless Sensor Networks", 2011 IEEE